REMARKS

The original application, filed October 31, 2003, included claims 1-35. An Office action of June 14, 2007, presented a restriction requirement with claims grouped as claims 1-11, 13-23, and 25-34 in Group I, and claims 12, 24, and 35 in Group II. In a Response to Restriction Requirement of July 6, 2007, Applicant elected to prosecute the claims in Group I, claims 1-11, 13-23, and 25-34, without traversal, wherein the claims of Group I were to be prosecuted alone (and the claims of Group II were to be correspondingly withdrawn).

In a second Office action of September 27, 2007, Examiner objected to claims 2, 14, 26 for minor informalities. Applicant responsively amended claims 2, 14 and 26 in accordance with Examiner's request. Examiner also objected to claims 6-8 on grounds that they had improper dependency numbering. Applicant responsively amended claim 1 to incorporate claims 6 and 8, canceled claims 6 and 8, and amended claim 7, thereby overcoming the objection.

The present Office action, which is dated March 3, 2008, is responsive to Applicant's amendment filed on December 27,2007, wherein Applicant amended claims 1,2,11,13,14,19,23,25,26,27,28,3 1,33,34 and canceled claims 5,6,8,17,18,29,30,32. Claims 1-4,7,9-11,13-16,19-23,25-28,3 1 and 33-34 are pending. Applicant gratefully acknowledges that the present Office action withdraws the previous rejections under 35 USC 101, 102(b) and 103(a), and 112.

The present Office action presents new grounds of rejection. Specifically, claims 1, 3-11,13,15-23, 25 and 27-34 stand rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication No. 200310101353 ("Tarquini") in view of US Patent No. 7,185,368 ("Copeland"), or possibly US Patent No. 6,851,061 ("Holland "). (Copeland is recited in the broad statement of the rejections, but Holland is recited in the detailed remarks.) Claims 2,14,26 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini in view Copeland, or possibly Holland. (Again, Copeland is recited in the broad statement of the rejections, but Holland is recited in the detailed remarks.) Claims 11, 23, and 34 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini in view of US Patent Publication No 2004101 17478 ("Triulzi").

To overcome the rejection, Applicant herein amends claims 1, 2, 7, 13, 14, 19, 20, 25, 26, and 31 and submits new claims 36-44.

Claims 1, 13 and 25

According to the present application, data packets are communicated from a transport layer to an application receive queue (ARQ) before being communicated from the ARQ to the ARQ's application, which is in the application layer. See present application, e.g., page 11, lines 18-19 (data is passed to ARQ and then to application layer); page 10, lines 12-16 (transport layer copies the data to ARQ, etc.); page 11, lines 26-28 and FIG. 7 (application 720 associated with ARQ 718).

Further according to the present application, a host-based network intrusion detection system (HNIDS) is provided and has the capability of accessing this communication to the ARQ, which is between the transport and application layers. See, e.g., present application, page 5, line 12 (HNIDS is "deployed"); page 9, lines 17-19 (scan daemon 300 of HNIDS has program code 302 enabling HNIDS scan daemon process 300 to monitor data packets that have been communicated to the ARQ, in one embodiment); page 10, lines 28-29 (HNIDS interfaces to the communication between transport layer 516 and ARQ 518, in one embodiment).

By this interfacing/monitoring capability, the HNIDS avoids promiscuous scanning and instead scans only data packets sent to the target system on which HNIDS is deployed. See present application, e.g., page 5, lines 13-16 (not promiscuous); page 6, lines 6-8 (HNIDS scans only the data to the target system). Further, for a particular application this scanning is still more targeted, since the HNIDS process scans data packets either enroute to the application's ARQ or that are already in its ARQ, as pointed out above.

HNIDS prevents processing of data packets by the application if they are determined to be malicious. See present application, e.g., page 11, lines 4-5 (bad data is not put into ARQ in one embodiment) and lines 23-28 (application is notified not to process bad data or is killed, according to alternatives, for example).

By contrast, Tarquini et al., the primary reference relied upon for the rejection, teaches that an intrusion prevention system (IPS) is provided above the *network* layer ("intermediate network filter service provider 140"), and, more specifically "at the

transport layer level." Tarquini, paragraph 40. Copeland or Holland are relied upon in the Office action for teaching about scanning between a transport and application layer. Applicant assumes the Office action intends to refer to Holland, since the detailed discussion of the rejection clearly corresponds to Holland, and since Copeland does not seem relevant.

An intrusion prevention system at the transport layer, as taught by Tarquini, is not *between* the transport and application layers. This is significant at least because neither Tarquini nor the combination of Tarquini and Copeland or Holland teach or suggest that data packets have been directed to a particular application's ARQ when an IPS checks them in a transportation layer. Neither Tarquini, nor Copeland, nor Holland have any reference at all to an application receive queue. Thus, the references do not teach or suggest scanning that is for particular data packets sent to an application's ARQ, which facilitates less promiscuous scanning and also facilitates taking an action to prevent the particular application from processing bad data packets.

To clearly point out these differences, claims 1, 13 and 25 of the present application have been amended herein to recite "accessing, by a network intrusion detection process of a target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system, wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the application from the transport layer . . . the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ . . . taking at least one action to prevent the application from processing data packets from the remote host to the application responsive to . . . determining that any of the scanned data packets are malicious." As explained herein above, Tarquini does not teach or suggest this. Nor does Tarquini in combination with Holland or Copeland.

Further, Applicant notes that the Office action relies upon Tarquini's teaching about a network stack to meet the previously recited features of an application receive queue. Applicant submits that Tarquini's network stack does not teach or suggest an application receive queue, particularly not one that is between a transport layer and

application layer, as in the present invention, as claimed.

Claims 2, 14 and 26

The Office action relies upon Tarquini paragraphs 40 and 41 for teaching regarding terminating an application responsive to detecting malicious data packets. Applicant has carefully read the relied upon passage and respectfully submits that the cited passage simply does not teach or even suggest this. All the more certainly, Tarquini does not teach or suggest taking an "action to prevent the application from processing data packets from the remote host to the application responsive to . . . determining that any of the scanned data packets are malicious" where the determining is of scanned data packets "directed to the application from a remote host via the communications network, and wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ" and where "the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the application from the transport layer," as now recited in the combination of claims 1 and 2, 13 and 14, and 25 and 26.

Claims 37, 40 and 43

The Office action relies upon Tarquini paragraph 48 for teaching regarding intimating the transport layer to tear down the remote host connection responsive to detecting malicious data packets. Applicant has carefully read the relied upon paragraph and respectfully submits that the cited paragraph simply does not teach or even suggest this. All the more certainly, Tarquini does not teach or suggest "wherein the directing of the data packets to the application from the remote host is via a connection with the remote host on the communications network, and wherein said . . . action includes intimating the transport layer to tear down the remote host connection, " the action being an "action to prevent the application from processing data packets from the remote host to the application responsive to . . . determining that any of the scanned data packets are malicious as now recited in the combination of claims 1 and 37, 13 and 40, and 25 and 43.

Claims 38, 41 and 44

Still more certainly, Applicant submits that the references do not teach or suggest that "after intimating the transport layer to tear down the remote host connection, the target computer services requests on connections other than that remote host connection." (Regarding support for this amendment, see present application, page 10, lines 1-5 and page 11, lines 6-8.)

Claims 3, 4, 7, 9, 10, 11, 15, 16, 19-23, 27, 28, 31, 33, 34, 36, 29, and 42

Applicant submits that claims 3, 4, 7, 9, 10, 11, 15, 16, 19-23, 27, 28, 31, 33, 34, 36, 29, and 42 are allowable at least because they depend on respectively allowable claims, as discussed herein above.

REQUESTED ACTION

Applicant submits that the claims as submitted herein are patentably distinct, and hereby requests that Examiner grant allowance and prompt passage of the application to issuance.

Respectfully submitted,

Anthony V. S. England
Attorney for Applicant
Registration No. 35,129
512-477-7165
a@aengland.com